

CLAIMS:

1. (Currently amended) A communication authorization method, comprising the steps of:

a third party server receiving a request for access information to access content;
generating the access information to access the desired content from a first application server;

generating authentication of the access information using a first service ticket to the first application server, wherein the first service ticket is obtained from a key distribution center; and

sending the access information and authentication to a client, whereby the client presents the access information and authentication to the first application server to be authorized to receive the desired content from the first application server.

2. (Canceled)

3. (Currently amended) The method as claimed in claim 1, wherein the step of generating the access information ~~including~~ includes generating session rights and encrypting at least a portion of the session rights using a third party server service key for the first application server.

4. (Previously presented) The method as claimed in claim 1, further comprising the step of:

generating at least a portion of the authentication using the first service ticket.

5. (Original) The method as claimed in claim 4, further comprising the steps of:
requesting a ticket granting ticket (TGT ticket);
receiving a TGT ticket;
requesting the third party server service ticket for the first application server; and
receiving the third party server service ticket for the first application server.

6. (Previously presented) The method as claimed in claim 1, further comprising
the steps of:

the application server receiving a key request including the access information
and authentication;
extracting the access information and authentication;
verifying the authentication of the access information using the first service ticket,
and client authorization; and
issuing a key reply if the authentication of the access information and client
authorization are verified.

7. (Original) The method as claimed in claim 6, further comprising the steps of:
a client generating a key request including the access information and the
authentication;
sending the key request to the first application server; and
receiving the key reply (KEY_REP) if the authentication of the access
information and client authorization are verified by the first application server.

8. (Currently amended) A method for verifying authorization for a client to gain access to content and/or services, comprising the steps of:

receiving a key request from a client;

extracting third party server access information and third party server authentication from the key request;

verifying an authentication of the third party access information and a client authorization; and

issuing a key reply if the authentication of the third party access information and the client authorization are verified.

9. (Original) The method as claimed in claim 8, further comprising the step of authenticating the third party server access information using the third party server authentication.

10. (Currently amended) The method as claimed in claim 9, wherein the step of authenticating includes extracting a first service ticket ~~from the authentication~~ and authenticating the third party server access information using the first service ticket.

11. (Currently amended) The method as claimed in claim 8, wherein the step of extracting the third party server authentication, further comprising the steps of extracting a session key from the key request; and the step of authenticating the access information ~~including~~ includes verifying a third party server signature using the session key.

12. (Currently amended) The method as claimed in claim 11, wherein the step of extracting the session key ~~including~~ includes decrypting at least a portion of the key request using an application server service key and extracting the session key.

13. (Previously presented) The method as claimed in claim 8, further comprising the steps of:

the third party server receiving a request for the access information to access content;

generating the third party server access information to access the desired content from a first application server; and

generating the third party server authentication of the access information.

14. (Currently amended) The method as claimed in claim 13, wherein the step of generating the third party server authentication ~~including~~ includes incorporating a third party server service ticket for the first application server.

15. (Currently amended) The method as claimed in claim 14, wherein the step of generating the authentication ~~including~~ includes generating a signature utilizing a session key of the third party server service ticket.

16. (Currently amended) The method as claimed in claim 14, wherein the steps of verifying the authentication of the access information ~~including~~ includes extracting the third party server service ticket and verifying the third party server service ticket.

17. (Previously presented) A method for providing secure communication when distributing services, comprising the steps of:

- a third party server receiving a selection for services;
- issuing access information for the services;
- issuing authentication of the access information;
- an application server receiving a key request from a client;
- verifying an authentication of the access information and a client authorization utilizing, at least in part, a first service ticket; and
- issuing a key reply to a client if the authentication of the access information and the client authorization are verified.

18. (Previously presented) The method as claimed in claim 17, further comprising the steps of:

- a KDC receiving a first service ticket request from a third party server for the application server;
- the KDC issuing the first service ticket to the third party server for the application server; and

the steps of the third party server issuing access information and authentication including generating the access information and authentication using the first service ticket.

19. (Previously presented) The method as claimed in claim 17, further comprising the steps of:

the KDC receiving a second service ticket request from a client for the application server;

issuing a second service ticket for the application server; and

the step of the application server receiving a key request from a client wherein the key request includes the second service ticket.

20. (Currently amended) The method as claimed in claim 17, wherein: the step of the application server verifying the authentication of the access information ~~including~~ includes:

extracting the first service ticket;

decrypting the first service ticket;

extracting a session key from the first service ticket;

generating a signature using the session key; and

verifying the signature over the access information with the session key.